CLAIMS

Claim:

1. A industrial network, comprising:

a local area network; and

a security policy implementation point (SPIP) configured to apply policy in the control of network access to at least one factory machine.

2. The industrial network of claim 1, further comprising a programmable logic controller connected to the at least one factory machine, and wherein the SPIP is integrated with the programmable logic controller.

3. The industrial network of claim 1, further comprising a programmable logic controller connected to the at least one factory machine, and wherein the SPIP interfaces between the local area network and the programmable logic controller.

4. The industrial network of claim 3, wherein the local area network is an Ethernet network, wherein the SPIP is configured to communicate with network devices on the local area network over the Ethernet network, and wherein the SPIP is configured to communicate with the programmable logic controller using a protocol selected from at least one of Profibus, Controller Area Network, RS-232, RS-422, and RS-485.

5. The industrial network of claim 1, wherein the local area network includes at least one Ethernet switch/router, and wherein the SPIP is included as a blade in the Ethernet switch/router.

6. The industrial network of claim 5, wherein the SPIP is configured to implement security policy to control network access to at least one PLC connected to the Ethernet switch/router through the SPIP.

7. The industrial network of claim 6, wherein the subnet includes at least one programmable logic controller is configured to control the operation of at least one of said factory machines.

8. The industrial network of claim 1, wherein the SPIP comprises an authentication module and an authorization module to control network access to said factory machine.

9. The industrial network of claim1, wherein the industrial network is an untrusted network configured to interconnect network services with a plurality of SPIPs associated with factory machines, and wherein the network services are configured to enable operation of the factory machines to be altered through the industrial network.

10. The industrial network of claim 1, wherein the SPIP includes a local policy configured to enable the SPIP to enforce network policy in connection with local accesses.

11. The industrial network of claim 10, wherein the local policy comprises:

a local access policy configured to require authentication and authorization of at least one of an user and an accessing electronic device for non-emergency attempts to access the SPIP, and

an alternate access policy configured to allow access to the SPIP and maintain an audit log attendant to a local attempt to access the SPIP.

12. The industrial network of claim 1, wherein the SPIP comprises a network policy configured to enable the SPIP to enforce network policy by interfacing with network services.

13. The industrial network of claim 12, wherein the SPIP comprises a local authentication policy and information associated with authorized users and indicative of authorization policy information associated with said at least one factory machine.

14. A Security Policy Implementation Point (SPIP) for use in an industrial network, comprising:

a local path configured to implement a local access policy; and

a network path configured to secure network paths on the industrial network.

15. The SPIP of claim 15, further comprising programmable logic controller circuitry configured to function to control at least one factory machine.

16. The SPIP of claim 15, wherein the local access policy includes enabling access to an associated factory machine to enable operation of the factory machine to be altered without verification of authorization and authentication of an user seeking to alter the operation.

17. The SPIP of claim 16, wherein the local path further comprises an accounting module configured to record accesses to at least one of the SPIP, an associated programmable logic controller, and an associated factory machine.

18. The SPIP of claim 15, wherein the local path comprises an authentication module configured to authenticate the identity of an individual seeking to access a device through the SPIP, and an authorization module configured to assess an authorization associated with the individual to ascertain whether the individual is authorized to access the device.

19. The SPIP of claim 18, wherein the authorization module is an interface to a Lightweight Directory Access Protocol (LDAP) server, and wherein the authentication module is an interface to a Remote Access Dial In User Service (RADIUS) server.

20. The SPIP of claim 18, wherein the authentication and authorization modules maintain a local copy of authorized users and authentication policy to allow local access to the SPIP.

21. The SPIP of claim 15, wherein the local path comprises a virtual private network module configured to participate in a virtual private network tunnel established on the industrial network.

22. The SPIP of claim 15, further comprising network ports configured to interface with the industrial network, and output ports configured to interface with a programmable logic controller.

23. The SPIP of claim 22, wherein the network ports are configured to communicate on the industrial network utilizing an Ethernet protocol; and wherein the output ports are configured to communicate with the programmable logic controller using a protocol understandable by the programmable logic controller.

24. The SPIP of claim 15, further comprising network ports configured to interface with the industrial network, control logic configured to implement a control program associated with a programmable logic controller, and interface ports configured to interface with a factory machine.

25. The SPIP of claim 24, wherein the interface ports comprise at least one input port configured to receive input from an environmental sensor, and at least one output port configured to control at least one electro-mechanical device.